

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 62-177696

(43)Date of publication of application : 04.08.1987

(51)Int.Cl.

G06K 19/00
B42D 15/02

(21)Application number : 61-018040

(71)Applicant : HITACHI LTD

(22)Date of filing : 31.01.1986

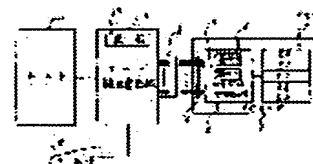
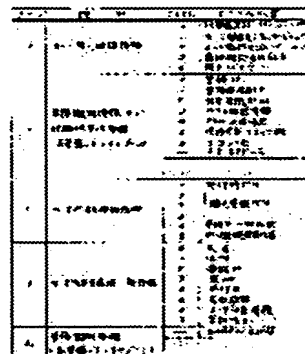
(72)Inventor : YAMASHITA KOTARO
KAWAOKA AKIHIRO
ASAMI KO

(54) MULTI-PURPOSE IC CARD AND METHOD TO USE

(57)Abstract:

PURPOSE: To apply a single IC card to plural works by comparing the collating result of identifying information and access conditions based on the contents of respective areas set to a memory and determining the permission or the rejection of an access request to the memory.

CONSTITUTION: In a memory 3 of an IC card 1, zones Z0WZ4 are included, and in respective zones, the information shown in the figure is stored. By a microprocessor 2, first, card identity confirming information sent from a card reading writing machine 7 is compared with the corresponding information in the card, and at the time of coincidence, the corresponding flag of a permission flag table 5 is set to '1'. Next, work identifying information is compared with corresponding information, and at the time of coincidence, the corresponding flag of the table 5 is set to '1'. Next, inputted identifying information PIN is coincident to a PIN in the memory, and then, the flag of a permission flag table 4 is set to '1'. Next, when an access request is executed, tables 4 and 5 are compared, the permission or the rejection of the request access action are investigated and in accordance with the result, execution or rejection is performed.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

⑨ 日本国特許庁(JP)

⑩ 特許出願公開

⑪ 公開特許公報(A)

昭62-177696

⑫ Int. Cl.⁴

識別記号

庁内整理番号

⑬ 公開 昭和62年(1987)8月4日

G 06 K 19/00
B 42 D 15/02
G 06 K 19/00

N-6711-5B

7008-2C

Q-6711-5B

審査請求 未請求 発明の数 2 (全9頁)

⑭ 発明の名称 多目的ICカード及びその使用方法

⑮ 特 願 昭61-18040

⑯ 出 願 昭61(1986)1月31日

⑰ 発 明 者 山 下 廣 太 郎 川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

⑱ 発 明 者 川 岡 明 宏 川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

⑲ 発 明 者 浅 見 香 川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

⑳ 出 願 人 株式会社日立製作所 東京都千代田区神田駿河台4丁目6番地

㉑ 代 理 人 弁理士 野 萩 守 外1名

明 細 書

1. 発明の名称

多目的ICカード及びその使用方法

2. 特許請求の範囲

1. マイクロプロセッサと前記マイクロプロセッサを介して外部からアクセス可能なメモリとを内蔵し、業務の履行に際して前記メモリへのアクセスが必要とされるカードにおいて、前記メモリは、登録された各業務に関する識別情報のための領域と、前記各業務の個別情報のための領域と、各業務の前記個別情報領域を規定する領域管理情報のための領域とを含むことを特徴とする、多目的ICカード。

2. 特許請求の範囲1において、前記領域管理情報は、各業務の個別情報領域の位置を示す情報と大きさを示す情報とを含む、多目的ICカード。

3. 特許請求の範囲1において、前記識別情報領域と領域管理情報領域は空き領域の一方の端から

始まり、前記個別情報領域は空き領域の他端から始まる。多目的ICカード。

4. 特許請求の範囲1において、前記メモリ内の情報の各項目は、前記マイクロプロセッサにより実アドレスに変換される統一的形式の論理アドレスを持つ、多目的ICカード。

5. 特許請求の範囲1において、前記メモリ内の情報へのアクセスの許可条件が各項目に対して別個に定められた、多目的ICカード。

6. マイクロプロセッサと前記マイクロプロセッサを介して外部からアクセス可能なメモリとを内蔵し、前記メモリが、登録された各業務に関する識別情報のための領域と、前記各業務の個別情報のための領域と、各業務の前記個別情報領域を規定する領域管理情報のための領域とを含む、多目的ICカードを使用して業務を履行する際に行なわれる、所定の識別情報を外部機器から前記マイクロプロセッサに入力するステップと、前記マイクロプロセッサにおいて前記入力識別情報とそれに対応する前記メモリ内の

特開昭62-177696(2)

識別情報とを照合してその結果を保持するステップと、前記メモリ内の情報のある項目へのアクセス要求を前記外部機器から前記マイクロプロセッサに入力するステップと、前記マイクロプロセッサにおいて前記メモリ内の情報の各項目につき予め定められたアクセス許可条件と前記照合結果とを比較して前記アクセス要求の許可否を決定するステップとを含むことを特徴とする、多目的ＩＣカードの使用方法。

3. 発明の詳細な説明

〔産業上の利用分野〕

本発明は、ＩＣカードに関し、特に、複数の目的又は業務（身分証明、入場管理、銀行取引、クレジット購買等）に共用されるＩＣカードと、その使用方法に関する。

〔従来の技術〕

ＩＣカードに関しては、特公昭53-6491号以下多くの発明や提案があるが、カードの利用領域については、マイクロプロセッサのデータ処理機能を利用する本人確認行為の域を出ないもの

であることである。しかし、この方法では、メモリ領域のむだが多く、予め定められた個数を越えた業務は、たとえ空き領域の総和が充分な容量に達していても、登録することができない。

本発明は、前記の問題を解決し、それにより、権限チェック条件、記録情報の形式と長さなどが大幅に異なる可及的多数の業務に共用しうる、多目的ＩＣカードを提供しようとするものである。

〔問題点を解決するための手段〕

本発明によるＩＣカード内のメモリは、特徴として、各業務に関する識別情報（例えば、業務識別コード、業務固有の顧客識別番号等）のための領域と、各業務の個別情報（例えば、取引履歴、特定業務専用の顧客管理情報等）のための領域と、各業務の個別情報領域を規定する領域管理情報（例えば、各領域の位置、大きさ等）のための領域とを含む。

また、前記ＩＣカードの使用方法は、特徴として、入力された識別情報とそれに対応するメモリ内識別情報を照合してその結果を保持するステッ

がほとんどである。また、適用業務に因しても、単一の業務への適用が主であって、複数の業務、特に、記録される情報の形態、アクセス条件などを異にする複数の業務での共用に対しては、特設の工夫がなされたようには見受けられない。

〔発明が解決しようとする問題点〕

１枚のカードを複数の業務に対して共用する場合に、権限チェックが各業務に独自の情報に基づいて行なえることが望ましい。ある一組の条件に関する権限チェックですべての業務における権限を認める方法では、適用業務の範囲に著しい制限を課さざるをえない。また、記録される情報の形式や長さも、一般に、業務によって大幅に異なるから、これらについての制約があったり、あるいは、その制約を除くために特殊な処理を必要とするのでは、至って不便である。更に、適用業務の個数も、メモリ容量の許す限り多いことが望ましい。単一のＩＣカードに複数の業務を登録するための常識的な方法は、メモリを予めいくつかの固定長領域に分割して、各領域を一つの業務に割当

ブと、メモリ内情報の各項目につき予め定められたアクセス許可条件と前記照合結果を比較してメモリ内情報へのアクセス要求の許可否を決定するステップとを含む。

〔作用〕

別個に記憶された各業務に関する識別情報は、個別の識別情報に基づく業務ごとの権限チェックを可能にする。また、各業務の識別情報領域に対する領域管理情報を利用することにより、長さや形式の異なる複数の業務の個別情報を、メモリ領域のむだなく密に配置することができ、したがって、メモリ容量の許す限り多数の業務を登録することができ、新業務の追加も容易である。更に、業務により長さや形式の異なる業務個別情報へのアクセスを、領域管理情報を用いるアドレス変換を介して、統一的な論理アドレスによって指定することができる。

また、カード使用に際して、識別情報入力とメモリ内の対応識別情報の照合結果を保持するステップにより、チェックを要する諸識別項目につい

特開昭62-177696(3)

ての合否のテーブルが形成され、この照合結果とメモリ内情報の各項目につき予め定められたアクセス許可条件とを比較してアクセス要求の許否を決定するステップにより、項目及びアクセス形態ごとに異なるアクセス権限の有無が、アクセス要求の都度個別にチェックされる。

〔実施例〕

本発明のICカードは、LSIとして形成されたマイクロプロセッサと不揮発性メモリ（例えば、EEPROM）を内蔵する。第1図はそのメモリに記憶される情報の一例を示す。メモリ内の情報は多数のアイテムからなり、これらのアイテムはいくつかのゾーンにまとめられる。

ゾーン0の内容は、カード身元確認情報であり、主にカードの正当性のチェックに用いられる。アイテム0はIC製造元ID（IDは識別情報の略語）と当該ICのバージョン番号であり、アイテム1はカード製造元IDと当該カードの製造バージョン番号であり、アイテム2はカード発行元IDと当該カードの発行バージョン番号であり、ア

イテム3は最終確認責任者IDであり、アイテム4は最終確認責任者のパスワードである。ICチップの作製時に、^{IC}製造元IDとバージョン番号（アイテム0）と、IC製造元における最終確認責任者IDとそのパスワード（アイテム3、4）が書き込まれる。次に、カードの作製時に、カード製造元IDとバージョン番号（アイテム1）が書き込まれるとともに、アイテム3と4は、カード製造元における最終確認責任者IDとそのパスワードにそれぞれ書き換えられる。最後に、カードの発行時に、カード発行元IDとバージョン番号（アイテム2）が書き込まれるとともに、アイテム3と4は、カード発行元における最終確認責任者IDとそのパスワードにそれぞれ書き換えられる。

ゾーン1は、取扱う業務にそれぞれ対応するいくつかのサブゾーンからなる。各サブゾーンの内容は、対応する業務についての業務識別情報と記録域管理情報からなり、業務識別情報は主に当該業務の履行権限のチェックに用いられ、記録域管理情報は対応する業務の個別情報（後述するゾ

ン4）のためのメモリ領域の管理に用いられる。アイテム0は業務IDであり、アイテム1は業務権限者IDである。業務は、例えば、特定銀行との取引、特定店での購買、特定地区への入出、特定機器の操作、特定サービスの享受などであり、業務権限者は、関連する特定の銀行、店、地区又は機器の管理者、サービス提供者などである。アイテム2の利用者識別番号は、各業務についてカード所有者に与えられた個々の識別情報で、例えば、銀行口座番号、顧客番号などである。アイテム3のホスト返送情報は、カード内情報の処理の開始が外部機器（カード読出装置又はホスト処理装置）から要求された時に、リターン情報として送出される情報であり、その内容は業務により異なる。アイテム4のPIN必須指定は、後述するゾーン4へのアクセスに対して、PIN（後述するゾーン2に書き込まれる本人確認用暗証コード）の一致を必須条件とするか否かを指定する情報である。アイテム5は、後述するゾーン4内で当該業務のために使用しうるブロックの個数であ

り、アイテム6はそのブロックの長さ（例えば、バイト数）である。これらのアイテムの他に、ゾーン1は、前述の使用しうるブロックのスタートアドレスを含む。スタートアドレスは、内蔵マイクロプロセッサにとってのみ意味がある内部管理情報であるから、アイテム番号を持たない。ゾーン1の情報は、それぞれの適用業務の登録時に書き込まれる。

ゾーン2の内容は、カード所有者確認情報であり、主に本人の確認のために用いられる。アイテム0はカード発行時に一応与えられるPIN（本人確認用暗証番号：Personal Identification Number）であり、アイテム1〜3はその後各人が任意に決定して書き込むPINである。各PINは、例えば、4〜10桁の10進数である。アイテム4は記憶されたPINと入力されたPINの不一致の累積数である。この情報は、例えば、後述するカードの有効性の決定に用いられることができる。アイテム5は同一のPINの連続使用の可否を指定する情報であり、それは、PINの連続使

特開昭62-177696(4)

用の可否を示すビットと、各PINが前回使用された結果一時的に無効にされているか否かを示すビット群を含む。同一PINの連続使用の拒否が指定されると、たとえ正しいPINであっても、同じPINを続けて入力したときには、PINの不一致として扱われる。この措置により、あるPINを他人に知られたときでもカードの盗用を防止することができる。アイテム0と5はカードの発行時に書込まれる。

ゾーン3は、カード所有者属性一般情報であり、全業務で共通に必要なとされる範囲の属性情報と、カードシステムの運用上必要な情報からなる。アイテム0は氏名、アイテム1は住所、アイテム2は電話番号、アイテム3はカードシステムでの客番号、アイテム4はカードの発行日、アイテム5はカードの有効期限である。アイテム6はユーザ（カード発行元）が必要に応じて書込む任意の情報である。アイテム7はカードの有効性を示す情報であって、例えば、ゾーン2のアイテム4に記録された累積不一致回数が所定値に達したときに、

アイテム番号又はゾーン番号とBSNからなる統一的な論理アドレスによって識別される。ゾーン0、2及び3の各アイテムは、固定長であり、予め定められたそれぞれのメモリ領域に格納される。ゾーン1は、全体としては可変長であるけれども、各アイテム、したがって各サブゾーンは固定長であるから、業務IDを指定してサーチすることができる。ゾーン4のデータは、格納位置、データ長等が業務によって異なるけれども、BSNが与えられれば、ゾーン1中のスタートアドレスとブロック長情報を用いて、指定されたブロックの突アドレスを決定することができる。論理アドレスから突アドレスへの変換は、内蔵マイクロプロセッサにより遂行される。

ゾーンとアイテムのメモリ内配置は、必ずしも第1図に示されたような整然としたものである必要はなく、一定のアルゴリズム又はテーブルに従って分散することにより、機密保護性を高めることができる。同じ目的で、記憶される情報にもシャッフル等の加工を施すことができる。長さが不足

カードが無効であることを示すように書替えられる。このゾーンはカードの発行時に書込まれ、アイテム6は当初は有効を示すコードである。

ゾーン4は、ゾーン1に登録されたそれぞれの業務に対応するサブゾーンからなり、各サブゾーンの内容は、対応する業務の個別情報、例えば、従来の磁気カードの記録情報、取引履歴、預金残高、非公開の顧客管理情報（勤務先、職位、年俸、資産等）、暗号キーなどであり、その性質により、業務登録時のまま固定され、あるいは、カードの使用の都度書込まれ又は更新される。このゾーンの情報は、ブロックと呼ばれる格納領域を単位としてアクセスされる。各業務における使用可能ブロック数及びブロック長はゾーン1のアイテム5及び6によりそれぞれ指定され、これら一連のブロックのスタートアドレスはゾーン1に管理情報として含まれている。各業務のための一連のブロックには、それぞれのBSN (Block Serial Number) が付与される。

メモリ内の情報は、対外的には、ゾーン番号と

のゾーン1及び4については、空きメモリ領域をその両端から順次各業務に割当てるのがよい。例えば、ゾーン1のサブゾーンには空き領域の先頭部分を割当て、ゾーン4のサブゾーンには空き領域の末尾部分を割当てる。あるいは、この逆でもよい。この割当アルゴリズムによれば、ゾーン1とゾーン4のためのそれぞれの領域を予め区分する必要がなく、メモリ容量の許す限り、任意の数の運用業務を登録又は追加することができる。

各ゾーンの各アイテムへのアクセス（読出し、書込み、消去）の許可条件は、各アイテムごとに、かつ、読出し、書込み、消去のそれぞれに対して、条件テーブルの形で任意に設定することができる。第2図は条件テーブルの一例を示す。図において、「読出し」、「書込み」、「消去」の各欄における0欄ないて4欄は、一致チェック項目を示し、0欄はゾーン0のアイテム3「最終確認責任者ID」、1欄は同ゾーンのアイテム4「最終確認責任者パスワード」、2欄はゾーン1のアイテム0「業務ID」、3欄は同ゾーンのアイテム1「業務権限

特開昭62-177696 (5)

者ID」、4欄はゾーン2のアイテム0～3のいずれか一つのPINに、それぞれ対応する(第5図参照)。これらの欄に記入された○印は、当該チェック項目の一致が対応アイテムへのアクセスの条件として設定されていることを表わす。同一アイテムに対する複数の○印は、それらのチェック項目の論理和がアクセス条件となることを示す。例えば、ゾーン0のアイテム0～2の読出しは、最終確認責任者ID又は同パスワードの一方が一致すれば可能であるが、同ゾーンのアイテム3の読出しは、最終確認責任者パスワードが一致した場合のみ可能であり、同ゾーンのアイテム4の読出しは不可能である。ゾーン0の消去は、カード発行後は不可能である。ゾーン4に対するアクセス条件欄中の△印は、そのチェック項目の一致によるアクセス許可が、ゾーン1のアイテム4においてPIN必須指定がなされていない場合のみ有効になることを表わす。このような条件テーブルは、内蔵マイクロプロセッサ内のROM又はメモリ中の特定領域に、ICの製造時に書き込ま

る。

第3図は、本発明のICカードとそのための処理システムを模式的に示す。ICカード1は、マイクロプロセッサ2と、それに接続された不揮発性メモリ(例えば、EEPROM)3とを内蔵する。マイクロプロセッサ2は、前述の条件テーブル(第2図)4と、後述する認可フラグテーブル(第5図)5とを備える。ICカードの使用にあたり、マイクロプロセッサの端子ピン6は、カード読出器7のソケット8に挿入される。カード読出器7は、PINその他の情報を入力するためのキーボード9と、ガイダンスその他の情報を表示するための表示装置10を有する。業務によっては、カード読出器10はホストコンピュータ11に接続されてもよい。

カード読出器7又はホストコンピュータ11とICカード内のマイクロプロセッサ2の間で伝送されるコマンド及びデータは、すべての処理について、第4図に示されるフォーマットのメッセージの形をとる。第4図において、FHはメ

ッセージの先頭を示すフィールドヘッダ、Cはコマンド、Zはゾーン番号、i又はBSNはアイテム番号又はBSN、BCCはブロックチェックコード、FEはメッセージの末尾を示すフィールドエンドコードである。i又はBSNのフィールドに空白コードがセットされたときは、ゾーン又はサブゾーンの全体が指定されたものと解釈される。

カード1がソケット8に挿入されて処理が開始されると、ホストコンピュータ11又はカード読出器7から送られた適当なコマンドに従い、第2図に示された条件テーブル上の各チェック項目0～4が一致するか否かが、マイクロプロセッサ2によりチェックされ、その結果が、認可フラグテーブル5に書き込まれる。第5図は、認可フラグテーブル5の内容の一例を示す。最終確認責任者IDとそのパスワード、通用業務に対する業務IDと業務権限者ID、又はPINが一致すれば、対応する位置0～4の認可フラグが“1”にセットされる。認可フラグテーブルの内容は、メモリ内の情報へのアクセス要求の可否を決定する時に

条件テーブルの内容と比較される。

第6図は、アクセス要求の可否を決定するためにマイクロプロセッサ2が遂行する処理のフローチャートである。カードがソケット8に挿入された後、カード読出器7又はホストコンピュータ11からの初期化コマンドを受けて、マイクロプロセッサ2による処理が開始される。まず、カード読出器7から送られたカード身元確認情報(例えば、最終確認責任者ID及び/又はパスワード)がカード内の対応情報と比較され、一致すれば、認可フラグテーブル5の対応フラグ(0,1)が“1”にセットされる(21)。カード身元確認情報は、カード読出器7又はホストコンピュータ11に予め固定的にセットされていてもよい。他の方法として、メモリ3内のゾーン1のアイテム3～4の内容に一定の相互関係を持たせておき、その関係が充たされているか否かを、マイクロプロセッサ2の内部処理のみによってチェックしてもよい。以後、この形のチェックを内部チェックと呼ぶ。

特開昭62-177696(6)

次に、カード読出書込機7又はホストコンピュータ11から送られた業務識別情報(例えば、業務ID及び/又は業務権限者ID)がカード内の対応情報と比較され、一致すれば、認可フラグテーブルの対応フラグ(2,3)が"1"にセットされる(22)。業務識別情報も、カード読出書込機7又はホスト11に固定的にセットされているともよい。

履行しようとしている業務に対してPIN必須指定(ゾーン1のアイテム4)が設定されている場合は、次に本人チェック(23)が行なわれる。すなわち、キーボード9から入力されたPINが、ゾーン2のアイテム0~3のPINのどれかと一致するか否かが調べられる。この時、ゾーン2のアイテム5が調べられ、PINの連続使用が許されていない場合には、入力されたPINがその時点で無効にされているか否かも併せて調べられる。その結果、入力されたPINとメモリ内の有効なPINの一つが一致すれば、認可フラグテーブルの位置4のフラグが"1"にセットされる。

す情報とを、メッセージのデータ部に含む。これを受けたカード内マイクロプロセッサは、カードの正当性又は業務の適用性のチェック(第6図21又は22)を行なうとともに、ホスト返送情報(ゾーン1のアイテム3)を要求に応じて返送する。

CHK:

これは、識別情報(業務ID、PIN等)をデータ部に含み、それとメモリ内の指定されたアイテムとの一致性のチェックを要求する。ただし、ゾーン1及び5については、業務IDの一致が確認された後の当該業務のサブゾーンのみがチェックの対象となる。

WRT:

これは、データ部の内容のメモリへの書き込みを要求する。

RDD:

これは、メモリ内の情報の読出しを要求する。以下の説明において、コマンド略号に括弧内の語は、メッセージのゾーン番号部、アイテム

その後、カード読出書込機7又はホストコンピュータ11からメモリ内情報に対するアクセス(読出し、書き込み、消去)を要求するコマンドが送られると、マイクロプロセッサ2は、条件テーブル4と認可フラグテーブル5を比較して、対象アイテムに対して要求されたアクセス動作(読出し、書き込み、消去)が許可しうるか否かを調べ(24)、その結果に従って、要求されたアクセスを実行し(25)、あるいは拒否する(26)。

次に、前述のICカードが銀行預金業務と健康管理業務に適用された場合について、コマンドに従ったカード処理過程の例を説明する。ただし、カードの正当性のチェックは、適用業務設定過程を除き、カードの挿入により自動的に起動される前述の内部チェックにより果たされるものとし、かつ、次のコマンドが用意されているものとする。

INT:

これは、ICカードとの会話の開始を宣言する初期化コマンドであり、カード身元確認情報又は業務識別情報とホスト返送情報の有無を示

番号又はBSN部、及びデータ部の各内容を示す。記号"Z"はゾーン、"i"はアイテム、"-"は空白、"A"はカード発行元(VAN業者)の最終確認責任者、"B"は銀行預金業務、"C"は健康管理業務を、それぞれ表す。また、条件テーブルは第2図のように設定されているとする。

適用業務B及びCの登録は、次のようなコマンド列によって行なわれる。カード身元確認情報(ゾーン0)は既に書き込まれているとする。

(1) INT(Z0, i4, Aのパスワード)

このコマンドにより、カードとの会話が始まり、同時に、入力されたAのパスワードとゾーン0のアイテム4との一致性がチェックされ、その結果に従って、認可フラグ1がセットされる。ホスト返送情報は要求されない。

(2) WRT(Z1, -, BのZ1情報)

アイテム番号は指定されず、データ部の内容は銀行預金業務に対してゾーン1に設定すべき全アイテムであり、これらも一つのサブゾーンとして書き込まれる。ホスト返送情報(i3)と

特開昭62-177696(7)

して口座番号と暗証番号と次に書込むべきブロックのBSNとが指定され、PIN必須指定(i4)がセットされ、使用可能ブロック数(i5)は"10"、ブロック長(i6)は32バイトであるとする。

(3) WRT(Z1, -, CのZ1情報)

このコマンドにより、前記と同様に、健康管理業務に対するゾーン1の全アイテムが書込まれる。ホスト返送情報は空白であり、PIN必須指定はなく、使用可能ブロック数は"1"で、ブロック長は56バイトとする。

銀行預金業務における取引に際してのコマンドシーケンスは、例えば、次のとおりである。

(1) INT(Z1, i0, BのID・ホスト返送情報要求)

このコマンドにより、業務の適用性のチェック(第6図22)が業務IDについて行なわれ一致すれば、認可フラグ2がセットされるとともに、ホスト返送情報として、口座番号と暗証番号と次に書込むべきブロックのBSNとが、

クを示すBSNを含む更新されたホスト返送情報が、ゾーン1のアイテム3としてセットされる。

次に、健康管理業務における情報読出しのためのコマンドシーケンスの例を示す。

(1) INT(Z1, i1, CのID)

このコマンドにより、業務IDがチェックされ、一致すれば認可フラグ2がセットされる。ホスト返送情報は用意されていない。カード正当性チェックは自動内部チェックにより完了している。

(2) RDD(Z4, -, -)

健康管理業務のためのゾーン4は単一のブロックからなるので、BSNを指定する必要はない。PIN必須指定はセットされていなかったから、INTコマンドに応じて行なわれた業務IDのチェックにより認可フラグ2がセットされていさえすれば、健康管理に関するゾーン4の情報(病歴、医学的特徴等)を読出すことができる(第2図△印参照)。

カード読出番込機7に送られる。なお、カード正当性チェックは、前述のように、自動内部チェックにより完了している。

(2) PINの入力

PINの入力を促すガイダンスが表示され、カード使用者は、キーボード9を用いて、PINを入力する。

(3) CHK(Z2, -, PIN)

このコマンドにより、本人チェック(第6図23)が行なわれ、入力されたPINとメモリ内のPINのどれかが一致すれば、認可フラグ4がセットされる。その後、

(4) WRT(Z4, BSN, 取引データ)

このコマンドにより、取引(預金引出し、入金等)に関するデータが、ホスト返送情報により指定されたBSNを持つブロックに書込まれる。

(5) WRT(Z1, i3, 更新されたBSNを含む新ホスト返送情報)

このコマンドにより、次に書込むべきブロッ

クを示すBSNを含む更新されたホスト返送情報が、ゾーン1のアイテム3としてセットされる。

[発明の効果]

本発明によれば、各業務に対する権限チェックを個別に行なうことができ、また、データの形式や長さの異なる多種多様な業務に関する情報をメモリ容量のむだなく記録することができ、かつ、すべての情報へのアクセスを統一的な論理アドレスを用いて行うことができる。したがって、単一ICカードの複数業務への適用が容易になる。

4. 図面の簡単な説明

第1図は本発明によるICカード内のメモリの内容の一例を示す図、第2図は第1図に示されたメモリ内容へのアクセス許可条件を定める条件テーブルの一例を示す図、第3図は本発明によるICカード及びそれが適用されるカード処理システムのブロックダイアグラム、第4図はカード内の

特開昭62-177696(8)

第 1 図

マイクロプロセッサと外部機器の間で伝送される
コマンドのフォーマット図、第5図は識別情報の
照合の結果形成される認可フラグテーブルの一例
を示す図、第6図はカード内のマイクロプロセッサ
によるアクセス許可決定処理のフローチャート
である。

1…ICカード、2…マイクロプロセッサ、3
…メモリ、20～24…情報ゾーン、4…条件テ
ーブル、5…認可フラグテーブル、7…カード読
出装置、9…キーボード、11…ホストコンピ
ュータ。

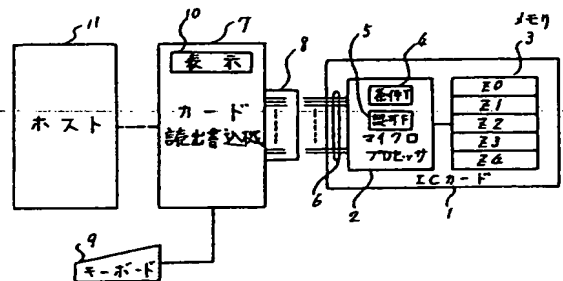
代理人 井理士 野 萩 守
(ほか1名)

ゾーン	種 別	アイテム	アイテム内容
0	カード身元確認情報	0	IC製造元ID、バージョンNo
		1	カード製造元ID、バージョンNo
		2	カード発行元ID、バージョンNo
		3	最終確認責任者ID
1	業務識別情報 及び 記録域管理情報 (各業務ごとにサブゾーン)	4	同上パスワード
		0	業務ID
		1	業務確認者ID
		2	利用者識別No
		3	ホスト返送情報
		4	PIN必須指定
		5	使用可能プロット数
2	カード所有者確認情報	6	プロット長
		7	スタートアドレス
		0	発行時PIN
		1	個人登録PIN
		2	登録不一致回数
3	カード所有者属性一般情報	3	PIN連続使用可否
		4	氏名
		5	住所
		6	電話番号
		7	営業No
		8	発行日
		9	有効期限
4	業務個別情報 (各業務ごとにサブゾーン)	10	有効性情報
		11	有効性コード

第 2 図

ゾーン	アイテム	アイテム内容	種 別	種 別	種 別
			0 1 2 3 4	0 1 2 3 4	0 1 2 3 4
0	0	IC製造元ID、バージョンNo	○	○	○
	1	カード製造元ID、バージョンNo	○	○	○
	2	カード発行元ID、バージョンNo	○	○	○
	3	最終確認責任者ID	○	○	○
1	4	同上パスワード	○	○	○
	0	業務ID	○	○	○
	1	業務確認者ID	○	○	○
	2	利用者識別No	○	○	○
	3	ホスト返送情報	○	○	○
	4	PIN必須指定	○	○	○
	5	使用可能プロット数	○	○	○
2	6	プロット長	○	○	○
	7	スタートアドレス	○	○	○
	0	発行時PIN	○	○	○
	1	個人登録PIN	○	○	○
	2	登録不一致回数	○	○	○
3	3	PIN連続使用可否	○	○	○
	4	氏名	○	○	○
	5	住所	○	○	○
	6	電話番号	○	○	○
	7	営業No	○	○	○
	8	発行日	○	○	○
	9	有効期限	○	○	○
4	10	有効性情報	○	○	○
	11	有効性コード	○	○	○

第 3 図



第 4 図

FH	C	E	L	データ	BCC	FE
----	---	---	---	-----	-----	----

第 5 図

フラグ位置	最終確認責任者		適用業務		PIN
	ID	パスワード	業務ID	業務確認者ID	
0	1	2	3	4	

特開昭62-177696 (9)

第6図

